

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
7 octobre 2004 (07.10.2004)

PCT

(10) Numéro de publication internationale
WO 2004/086663 A2

(51) Classification internationale des brevets⁷ : **H04K 1/00**

(21) Numéro de la demande internationale :
PCT/FR2004/000672

(22) Date de dépôt international : 19 mars 2004 (19.03.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
03/03803 24 mars 2003 (24.03.2003) FR

(71) Déposant (pour tous les États désignés sauf US) :
SAGEM S.A. [FR/FR]; Le Ponant de Paris, 27, rue
Leblanc, F-75512 Paris Cedex 15 (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : LEMASSON,
Eric [FR/FR]; 61, allée des Gentianes, F-95180 Menucourt
(FR).

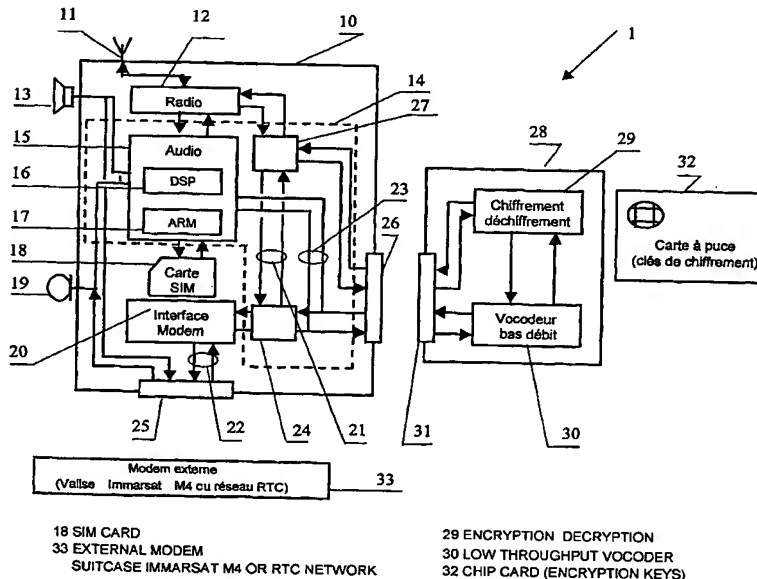
(74) Mandataire : DEBAY, Yves; Cabinet Debay, 126, Elysée
2, F-78170 La Celle St-Cloud (FR).

(81) États désignés (sauf indication contraire, pour tout titre de
protection nationale disponible) : AE, AG, AL, AM, AT,
AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,
CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG,
KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,
MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,

[Suite sur la page suivante]

(54) Title: TELEPHONE COMMUNICATION SYSTEM

(54) Titre : SYSTEME DE COMMUNICATION TELEPHONIQUE



(57) Abstract: A telephone communication system comprising a radiocommunication module (10) and a data encryption/decryption module (28), characterized in that the radiocommunication module (10) comprises a modem interface module (20) which is connected to the radiocommunication module (10) and controls an external modem (33). The encryption/decryption module (28) comprises a microcircuit support reader, an encryption/decryption circuit (29) and a vocoder circuit (30) receiving voice data to be encrypted or decrypted from the communication module (10). The encryption/decryption (29) of data is carried out directly in the encryption/decryption circuit (29) of the encryption/decryption module.

(57) Abrégé : Système de communication téléphonique comprenant un module de radiocommunication (10) et un module de chiffrement/déchiffrement (28) des données, caractérisé en ce que : le module de radiocommunication (10) comprend un module d'interface modem (20) relié au module de

[Suite sur la page suivante]



PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

- (84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

- sans rapport de recherche internationale, sera republiée dès réception de ce rapport

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

radiocommunication (10) et pilotant un modem externe (33), le module de chiffrement/déchiffrement (28) comprend un lecteur de support à micro circuit, un circuit de chiffrement/déchiffrement (29) et un circuit vocodeur (30) recevant des données voix à chiffrer ou à déchiffrer du module de radiocommunication (10), le chiffrement/déchiffrement des données étant effectué directement dans le circuit de chiffrement/déchiffrement (29) du module de chiffrement/déchiffrement (28).

Système de communication téléphonique

DOMAINE TECHNIQUE DE L'INVENTION

La présente invention concerne un système de communication téléphonique offrant à son utilisateur la possibilité de choisir plusieurs modes de communication avec son correspondant. On entend par ici une
5 de communication en clair ou chiffrée de la voix ou de données.

La présente invention vise notamment à autoriser de telles communications dans toutes zones géographiques couvertes ou non par un réseau de radiophonie cellulaire.

10 ARRIERE-PLAN TECHNOLOGIQUE DE L'INVENTION

Il est connu dans l'art antérieur des téléphones fixes ou mobiles qui utilisent une communication cryptée afin de protéger des conversations de bout en bout du réseau. Ces téléphones nécessitent un appareil ou une extension qui permet de réaliser ce chiffage. Il est nécessaire que les deux
15 interlocuteurs d'une conversation chiffrée aient en possession un outil de chiffage déchiffage des données.

Plus particulièrement, les téléphones mobiles ont besoin d'une technologie discrète et facile d'utilisation. Il est connu par le brevet EP 0 818 937 A1, un équipement de communication radio téléphonique qui permet de
20 crypter une conversation et utilisé le canal de transmission de données. Cet équipement comprend un téléphone mobile de type GSM comportant un microphone et un écouteur. Ce téléphone est raccordé, par une connexion filaire, à une unité d'extension qui réalise le chiffage de la conversation. L'unité d'extension a un aspect extérieur semblable à celui d'un terminal de
25 radio communication et comporte au moins un vocodeur et un module de chiffrement. Dans un mode de communication sécurisé, le vocodeur forme à partir du signal issu du microphone un flux binaire que le module de chiffrement traite pour produire des données envoyées à une interface de données, vers le terminal, pour transmission sur un canal de données. En
30 réception, des données présentées à l'interface de données après réception

sur un canal de données sont déchiffrées par le module de chiffrement pour produire un flux binaire que le vocodeur décode pour commander l'écouteur. Ce brevet exploite ainsi la présence de canaux de données dans certains réseaux de radiotéléphonie.

5 Il est connu par le brevet FR 2 809 920 un téléphone mobile comportant un terminal de communication radio téléphonique dont le capot anti-poussière est modifié. Ce capot comprend un lecteur de support à microcircuit permettant d'insérer une carte à puce pouvant servir au cryptage des données. Dans le cas où les données devraient être sécurisées, un
10 programme de cryptage est prévu dans une mémoire programme de la carte à puce ou dans la mémoire programme du boîtier principal.

Les conversations ou communications cryptées à partir ou vers un téléphone mobile sont transmises par le biais du réseau de radiotéléphonie mobile.

15 Une autre utilisation du téléphone portable de type GSM est la transmission de données par la connexion d'un modem d'un ordinateur portable avec un téléphone mobile. Ainsi l'ordinateur pilote le téléphone mobile à travers son modem et peut transmettre vers l'extérieur ou recevoir des données de l'ordinateur par le réseau de radio communication. Un tel
20 dispositif est connu de la demande de brevet GB230343.

Cependant, lorsque l'utilisateur d'un téléphone mobile voyage dans un pays ou une région ne possédant pas de réseau de radiotéléphonie cellulaire, il ne peut utiliser son téléphone mobile soit à titre de modem, soit comme moyen de communication même si un réseau de téléphonie
25 commuté existe ou d'autres moyens de communication sont disponibles. Il n'existe pas à ce jour de possibilité de transmission de données chiffrées via le réseau de radiotéléphonie GSM.

DESCRIPTION GENERALE DE L'INVENTION

La présente invention a donc pour objet de pallier des inconvénients
30 de l'art antérieur en proposant un téléphone mobile pilotant un modem externe pour transmettre une conversation cryptée à travers le réseau RTC

(Réseau de Téléphonie Commuté) ou via une valise type Immarsat qui redirige les données vers un satellite. C'est le mode MODEM. La présente invention permet aussi la transmission de données cryptées lorsque le téléphone mobile est configuré en tant que transmetteur modem.

5 Ce but est atteint par un système de communication téléphonique comprenant un module de radiocommunication et un module de chiffrement / déchiffrement des données, caractérisé en ce que

- le module de radiocommunication comprend un module d'interface modem relié au module de radiocommunication et pilotant un modem
10 externe ;

- le module de chiffrement / déchiffrement comprend un lecteur de support à micro circuit, un circuit de chiffrement / déchiffrement et un circuit vocodeur recevant des données voix à chiffrer ou à déchiffrer du module de radiocommunication, le chiffrement / déchiffrement des données étant
15 effectué directement dans le circuit de chiffrement / déchiffrement du module de chiffrement déchiffrement.

Selon une autre particularité, le module de radiocommunication comprend un premier aiguillage des données voix cryptées vers l'interface modem ou vers un circuit de modulation / démodulation, constitué par un
20 moyen de commutation commandé par logiciel.

Selon une autre particularité, le module de radiocommunication comprend un second aiguillage des données du modem vers le module de chiffrement / déchiffrement ou vers un circuit de modulation / démodulation, constitué par un moyen de commutation commandé par logiciel.

25 Selon une autre particularité, le module de radiocommunication comprend au moins une commande du menu affiché, sur un moyen d'affichage du terminal, permettant de choisir le mode de conversation et de transmission.

Selon une autre particularité, le module de
30 chiffrement / déchiffrement est inséré dans un boîtier capot relié au module terminal par un contacteur.

Selon une autre particularité, le module de chiffrement / déchiffrement comporte un lecteur de support de données pour l'échange uniquement de clés de session de chiffrement de l'utilisateur.

Selon une autre particularité, le module de radiocommunication
5 comporte une connexion série vers un modem externe.

Selon une autre particularité, le système de communication téléphonique est caractérisé en ce que la connexion série est filaire de type RS232.

Selon une autre particularité, la connexion série est non filaire.

10 Selon une autre particularité, la connexion série non filaire est Infrarouge.

Selon une autre particularité, la connexion série non filaire est radio 802.11 (WIFI).

Selon une autre particularité, la connexion série non filaire est
15 bluetooth.

Selon une autre particularité, le mode de conversation sélectionné par le menu est une communication téléphonique en clair à travers le réseau de radiotéléphonie cellulaire, mettant en liaison directement un DSP en émission ou en réception avec un circuit de modulation démodulation radio
20 du module de radiocommunication.

Selon une autre particularité, le mode de conversation sélectionné par le menu est une communication téléphonique cryptée à travers le réseau de radiotéléphonie cellulaire, ce mode intercalant par la commutation du premier aiguillage entre un DSP et un circuit de modulation / démodulation
25 radio du module de radiocommunication le module de chiffrement / déchiffrement.

Selon une autre particularité, le mode de conversation sélectionné par le menu est une communication téléphonique cryptée à travers le réseau de téléphonie commuté ou un satellite via un modem externe commandé par
30 le module de radiocommunication, ce mode intercalant, par la commutation du premier aiguillage, entre le DSP et le module de chiffrement / déchiffrement, un circuit vocodeur adaptant les signaux

numériques du DSP à la vitesse de transmission d'un modem avant de les envoyer au circuit de chiffrement / déchiffrement et déroutant les signaux provenant du modem externe en sortant du circuit de chiffrement déchiffrement vers un haut-parleur et ceux provenant d'un microphone et
5 sortant du circuit de chiffrement / déchiffrement vers le modem externe.

Selon une autre particularité, le mode de transmission des données sélectionné par le menu est une transmission téléphonique en clair à travers le réseau de radiotéléphonie cellulaire mettant en liaison, par la commutation du second aiguillage, le module d'interface modem avec un circuit de
10 modulation démodulation radio.

Selon une autre particularité, le mode de transmission des données sélectionné par le menu est une transmission téléphonique cryptée à travers le réseau de radiotéléphonie cellulaire intercalant, par la commutation du second aiguillage, entre le module d'interface modem et le circuit de
15 modulation / démodulation radio, le module de chiffrement / déchiffrement.

BREVE DESCRIPTION DES DESSINS

D'autres particularités et avantages de la présente invention apparaîtront plus clairement à la lecture de la description ci-après, faite en référence aux dessins annexés, dans lesquels :

20 - la figure 1 représente un équipement de communication selon l'invention ;

- la figure 2 représente le diagramme synoptique d'un boîtier principal de communication et d'un module de chiffrement selon l'invention ;

25 - la figure 3A représente le diagramme synoptique du trajet de la voix lors d'une communication en clair ;

- la figure 3B représente le diagramme synoptique du trajet des données lors d'une communication en clair ;

30 - la figure 4A représente le diagramme synoptique du trajet de l'émission et de la réception de la voix lors d'une communication cryptée fonctionnant sur tous les réseaux GSM ;

- la figure 4B représente le diagramme synoptique du transfert de données lors d'une communication cryptée fonctionnant sur tous les réseaux GSM ;

5 - les figures 5A et 5B représentent respectivement le diagramme synoptique du trajet de l'émission et de la réception de la parole lors d'une communication cryptée sur tous les réseaux filaires et/ou satellite (mode MODEM) ;

- la figure 6 représente le diagramme synoptique d'une carte SIM.

10 DESCRIPTION DES MODES DE REALISATION PREFERES DE L'INVENTION

La figure 1 représente un téléphone mobile (1) relié à un modem externe (3) via une connexion série (2) par exemple filaire ou non filaire notamment de type radio 802.11 ou bluetooth ou infrarouge. Le modem (3) est relié au réseau de téléphonie commuté (RTC) (4) ou à une valise type
15 Immarsat (5) qui communique par ondes radio avec un satellite (6), ce dernier retransmet les informations vers le réseau RTC (4). Avec le téléphone (1) selon l'invention, si l'utilisateur est dans une zone non couverte par le réseau de radiotéléphonie cellulaire, il peut utiliser l'invention pour communiquer par l'interface modem du téléphone de manière cryptée ou non
20 avec une tierce personne via, par exemple le réseau téléphonique commuté.

La figure 2 montre un téléphone mobile (1) comprenant un boîtier de radiocommunication principal (10) et un module de chiffrement (28).

Le téléphone mobile comporte un circuit en bande de base (14) qui comprend :

25 - un module audio (15) comportant deux microprocesseurs. Un microprocesseur de traitement de signaux numériques type DSP (16), il permet la fonction vocodeur et adapte le débit des données au réseau GSM (13 000 bauds). Ce microprocesseur DSP (16) effectue un traitement des données et permet de mettre en forme des trames AMRT (accès multiple par
30 répartition dans le temps). Le module audio comprend un microprocesseur de type ARM (17) équivalent à un processeur RISC (Reduced Instruction Set

Computer) qui permet d'accroître les performances du système en utilisant un jeu d'instructions réduit. Ce microprocesseur gère l'ensemble du téléphone, par exemple l'affichage à l'écran, la gestion du clavier numérique, les différents menus de programmation, la connectique logicielle du circuit
5 bande de base GSM (14) ;

- un module d'interface modem (20) est relié au module radio (12) par un bus de données (21), pour lui fournir des données à émettre selon un canal de donnée du réseau radio, et pour transmettre vers une unité d'entrée / sortie de données (modem et/ou micro-ordinateur), des données
10 démodulées après réception sur un canal de données du réseau radio. Ce module d'interface modem (20) redirige les données via un connecteur série (25) par exemple de type RS232, vers un accessoire externe par exemple un modem externe (33) ou un ordinateur portable ;

- un moyen de commutation logiciel (27) permet l'aiguillage des
15 données voix cryptées, soit vers le module radio pour effectuer un transfert vers le réseau cellulaire, soit vers le module interface modem pour effectuer un transfert vers, par exemple, le réseau RTC ;

- un moyen de commutation logiciel (24) permet l'aiguillage des données data provenant par exemple d'un ordinateur portable via un modem
20 externe, soit vers le module radio pour transmettre de façon claire les données data vers le réseau GSM, soit vers le module de chiffrement / déchiffrement (28) qui va chiffrer les données data avant de les renvoyer vers le module radio (12).

Le téléphone mobile comprend aussi :

- 25 - un module radio (12) modulant et démodulant les signaux d'informations vers une antenne (11), qui envoie ou reçoit des données de ou vers l'extérieur. (Le module radio 12 est en dehors du circuit bande de base 14 voir figure 2) ;

- un microphone (19) qui permet de retransmettre de manière
30 analogique la voix ;

- un écouteur (13) qui convertit un signal analogique en un son ;

- un connecteur de carte SIM (non représenté) en contact avec une carte SIM (18) ;

- une carte SIM (18) qui comporte des éléments caractérisant la relation existant entre un opérateur de téléphonie mobile et un utilisateur du téléphone mobile. La figure 6 représente le diagramme synoptique de la carte Sim qui comprend un microprocesseur (180) une mémoire programme (181), une mémoire de données (182) reliées entre eux par l'intermédiaire d'un bus (183) ;

- une batterie (non représentée) rechargeable qui alimente le téléphone (10) et le module de chiffrement (28) ;

- un connecteur module de chiffrement (26) qui permet de transmettre les données en clair ou cryptées de ou vers le boîtier de chiffrement (28) via un lien DAI (Digital Audio Interface) (23) ;

- un connecteur série (25) filaire ou non filaire qui permet par exemple de recharger la batterie ou de transférer les informations entre le téléphone (10) et un modem externe (33). Ce connecteur comprend plusieurs entrées sorties dont deux (22) sont dédiées à la transmission des données entre un modem extérieur et l'interface modem, les autres sont reliées à l'écouteur, le microphone, et un dernier vers le module audio.

Le module de chiffrement (28) comprend :

- Un connecteur de module de chiffrement (31) qui permet de relier le module de chiffrement / déchiffrement au boîtier terminal (10) par un lien DAI (Digital Audio Interface) (23). Ce dernier comprend 4 fils pour la communication entre les deux boîtiers en émission réception vers le vocodeur (30) ou le circuit de chiffrement / déchiffrement (29). Ce connecteur (31) est en contact avec un connecteur identique (26) du boîtier terminal (10) ;

- un connecteur de lecteur de carte à puce (non représenté) qui comporte des palpeurs destinés à venir en contact avec des métallisations de la puce d'une carte à puce (32) ;

- un circuit de chiffrement / déchiffrement des données (29) relié au connecteur précédemment cité ;

- un vocodeur bas débit (30) qui effectue une numérisation / dénumérisation des données, pour les adaptées au débit Data (9 600 bauds) quand les données doivent transiter par le réseau RTC, par exemple.

5 Une carte à puce (32) que l'on peut insérer dans la fente de lecture de carte à puce du module de chiffrement peut être une carte de chargement ou de sauvegarde de clés de chiffrements dans un chiffrement à clés secrètes. Dans le cas d'un chiffrement à clés publiques, la carte à puce est une enceinte sécurisée pour élaborer une clé de session fournie au module
10 de chiffrement à chaque communication. Cette carte (32) évite de télécharger les éléments secrets d'un utilisateur dans le téléphone portable (10), ce qui le rend vulnérable. En effet, dès que les clés sont chargées, elles restent à l'intérieur.

Pour la mise en service du téléphone portable, l'utilisateur compose
15 un numéro, dit code PIN, sur le clavier de son téléphone. Ce code est transmis à la carte SIM (18) grâce à un programme de mise en service du module audio. Une fois le code PIN transmit à la carte SIM, un programme est exécuté sous l'ordre du microprocesseur (180) de la carte SIM (18). Dans la mémoire programme (181), le code PIN est comparé à un code mémorisé
20 dans une mémoire (182) de la carte SIM (18). Si la comparaison est positive, la mise en service du téléphone est autorisée et l'utilisateur peut sélectionner le mode de fonctionnement pour la communication.

En se référant aux techniques antérieures deux types de données à communiquer sont possibles : les données voix traitées par le module audio
25 et les données data provenant d'un accessoire externe, par exemple d'un ordinateur portable utilisant le téléphone comme un transmetteur modem.

Trois manières de transférer les données voix sont possibles, grâce à l'invention : une conversation standard en clair par le biais du réseau de radiotéléphonie mobile, une conversation cryptée par le biais du réseau de
30 radiotéléphonie mobile et une conversation cryptée (mode MODEM) par le biais d'une interface modem (20) pilotée par le téléphone portable (1) vers un réseau de communication filaire et/ou un réseau de communication par

satellites. Les deux premiers modes de conversations sont déjà connus. Le troisième mode de conversation concerne l'invention.

Le transfert des données data, par exemple, d'un ordinateur portable peut se faire de deux façons possibles : un transfert en clair des données data via le réseau GSM et un transfert en crypté des données data via le réseau GSM. Le premier mode de transfert est déjà connu, le second concerne une particularité de l'invention.

L'utilisateur a au préalable sélectionné, grâce à des moyens interactifs de son téléphone GSM, le mode de fonctionnement pour les cinq possibles correspondances aux explications ci-après. Ces moyens interactifs sont par exemple un bouton haut-bas, qui une fois actionné par l'utilisateur, fait apparaître dans la rubrique souhaitée du menu d'utilisation du téléphone le choix : Appel voix GSM en clair, Appel voix GSM en crypté, Appel voix Modem en crypté, Appel data GSM en clair, Appel data GSM en crypté. L'utilisateur sélectionne le mode de fonctionnement de son choix en appuyant sur le bouton haut-bas pour amener un marqueur en vis à vis ou en coïncidence avec le choix, puis valide son choix par un bouton validation.

Lorsqu'un utilisateur veut téléphoner, il peut choisir l'une des trois communications, grâce au menu proposé sur son téléphone. Ce menu est géré par le microprocesseur par exemple de type ARM (17) du module Bande de Base 14). Lorsqu'un utilisateur répond à un appel, le mode de conversation n'est pas programmé via le menu, il est mis en place automatiquement. Le téléphone portable scrute l'émission de données provenant soit du réseau de radiotéléphonie cellulaire, soit d'un accessoire, par exemple le modem externe.

La figure 3A représente le trajet de la voix pendant une communication en clair à travers le réseau GSM. Lors d'une communication standard en clair, la voix provenant du microphone (19) est, en émission, numérisée par le microprocesseur DSP (16) du module audio (15) au débit usuel du réseau GSM (13 000 bauds). Le module radio (12) va moduler ce signal pour le transmettre vers l'extérieur à l'aide de l'antenne (11).

En réception, les données voix de l'extérieur arrivant à l'antenne (11) sont démodulées par le module radio (12), dénumérisées par le module audio (15), et envoyées vers l'écouteur (13).

La figure 3B représente le trajet des données data en émission et
5 réception standard en communication en clair. En émission les données data sont transférées du modem (33) vers le connecteur série (25), qui les redirige vers l'interface modem (20). Cette dernière envoie les données data au module radio (12) via le bus de donnée (21). L'aiguillage (24) s'enclenche
10 afin que les données data soient redirigées vers le module radio (12). Celui-ci va moduler ce signal pour le transmettre vers l'extérieur via l'antenne (11). En réception le module radio (12) reçoit des données data via l'antenne (11). Il les démodule et les envoie vers l'interface modem via l'aiguillage (24). L'interface modem (20) redirige les données vers le modem externe (33) et un ordinateur portable, via le connecteur série.

15 Dans ce mode de communication, c'est le modem qui pilote le téléphone portable pour transmettre des données data vers le réseau GSM. Lors du transfert des données data du modem (33) vers l'interface modem (20), le modem (33) envoie des commandes AT du protocole Hayes avec les données.

20 La figure 4A représente le trajet de la voix pendant une communication cryptée à travers le réseau GSM. Lors d'une conversation cryptée par le réseau GSM, la voix subit une première numérisation adaptée au débit type GSM par le microprocesseur DSP (16) du module audio (15). Les données voix numérisées sont envoyées vers le vocodeur (30) du
25 module de chiffrement / déchiffrement (28) par un bus DAI (Digital Audio Interface) (23). Le vocodeur (30) dans ce cas effectue un deuxième traitement sur les données voix pour les adapter au débit mode DATA de 9 600 bauds, il envoie les données vers le circuit de chiffrement / déchiffrement (29) qui les chiffre. Les données voix cryptées au débit GSM sont ensuite
30 envoyées au module radio (12) via le bus de donnée (21) « data bus », qui les transmet vers l'extérieur par l'antenne (11).

En réception des données voix cryptées arrivent à l'antenne (11). Le module radio (12) les transmet vers le module de cryptage (29), qui les déchiffre. Les données voix sont transmises par le vocodeur (30) au module audio (15) qui effectue une dénumérisation pour envoyer un signal
5 analogique à l'écouteur (13).

La figure 4B représente le trajet des données data cryptées en émission et réception à travers le réseau de téléphonie mobile. En émission les données data sont transférées du modem (33) vers le connecteur série (25), qui les redirige vers l'interface modem (20). Cette dernière envoie les
10 données data au module de chiffrement / déchiffrement (28) via l'aiguillage (24). Les données data sont envoyées vers le vocodeur (30) du module de chiffrement / déchiffrement (28). Le vocodeur (30) dans ce cas n'effectue pas de numérisation des données adaptée au débit mode DATA de 9 600 bauds, il envoie simplement les données vers le circuit de
15 chiffrement / déchiffrement (29) qui les chiffre. Les données data cryptées sont ensuite envoyées au module radio (12) via le bus de donnée (21) « data bus » et l'aiguillage (27), qui les transmet vers l'extérieur par l'antenne (11).

En réception, le module radio reçoit des données data via l'antenne (11). Il les démodule et les envoie vers le module de chiffrement via
20 l'aiguillage (27) et le bus de donnée (21). Le circuit de chiffrement / déchiffrement (29) déchiffre les données data cryptées et les transmet vers le vocodeur (30). Celui-ci redirige les données vers l'interface modem (20) via le connecteur (31) et l'aiguillage (24). L'interface modem (20) redirige les données data vers le modem externe (33) et l'ordinateur portable,
25 via le connecteur série (25).

Dans ce mode de communication, c'est le modem qui pilote le téléphone portable pour transmettre des données data vers le réseau GSM. Lors du transfert des données data du modem (33) vers l'interface modem (20), le modem (33) envoie des commandes AT du protocole Hayes avec les
30 données.

La figure 5A représente en émission le trajet de la voix pendant une communication cryptée à travers un réseau filaire et/ou satellites (en mode

MODEM). Lors d'une conversation cryptée en mode MODEM, la voix subit une première numérisation adaptée au débit type GSM de 13 000 bauds par le processeur de signal numérique DSP (16) du module audio (15). Les données voix numérisées sont envoyées par un bus DAI (23) vers le

5 vocodeur (30) du module de chiffrement / déchiffrement (28) contenu par exemple dans un boîtier capot. Le vocodeur (30) effectue une deuxième numérisation des données voix en adaptant leur débit au débit mode DATA par exemple de 9 600 bauds d'une interface modem et envoie ces données vers le circuit de chiffrement / déchiffrement (29) qui les chiffre. Les données

10 voix cryptées sont ensuite redirigées vers le module interface Modem (20) via le bus de donnée « data bus » (21). L'aiguillage (27) des données voix sur le bus de donnée vers le module interface modem (20) ou vers le module radio (12) est géré par le microprocesseur de type ARM (17). Le module interface modem (20) permet d'envoyer des commandes AT du protocole

15 Hayes et les données, au modem externe (33) via un connecteur série (25) par exemple de type RS232.

La figure 5B représente, en réception, des données voix cryptées provenant, par exemple, du réseau RTC qui sont envoyées du modem externe (33) vers le module interface modem (20) via le connecteur série

20 (25). Ce module (20) les redirige vers le circuit de chiffrement / déchiffrement (29), qui les déchiffre. Les données sont transmises vers le vocodeur (30) pour une première dénumérisation, et sont envoyées au module audio (15) qui effectue une deuxième dénumérisation avant de les envoyer au haut-parleur (13).

25

Il doit être évident pour les personnes versées dans l'art que la présente invention permet des modes de réalisation sous de nombreuses autres formes spécifiques sans l'éloigner du domaine d'application de l'invention comme revendiqué. Par conséquent, les présents modes de

30 réalisation doivent être considérés à titre d'illustration, mais peuvent être modifiés dans le domaine défini par la portée des revendications jointes, et l'invention ne doit pas être limitée aux détails donnés ci-dessus.

REVENDICATIONS

1. Système de communication téléphonique comprenant un module de radiocommunication (10) et un module de chiffrement / déchiffrement (28) des données, caractérisé en ce que

5 - le module de radiocommunication (10) comprend un module d'interface modem (20) relié au module de radiocommunication (10) et pilotant un modem externe (33) ;

 - le module de chiffrement / déchiffrement (28) comprend un lecteur de support à micro circuit, un circuit de chiffrement / déchiffrement (29) et un
10 circuit vocodeur (30) recevant des données voix à chiffrer ou à déchiffrer du module de radiocommunication (10), le chiffrement / déchiffrement des données étant effectué directement dans le circuit de chiffrement / déchiffrement (29) du module de chiffrement déchiffrement (28).

2. Système de communication téléphonique selon la revendication 1,
15 caractérisé en ce que le module de radiocommunication (10) comprend un premier aiguillage (27) des données voix cryptées vers l'interface modem (20) ou vers un circuit de modulation / démodulation (12), constitué par un moyen de commutation commandé par logiciel.

3. Système de communication téléphonique selon la revendication 1
20 ou 2, caractérisé en ce que le module de radiocommunication (10) comprend un second aiguillage (24) des données du modem vers le module de chiffrement / déchiffrement (28) ou vers un circuit de modulation / démodulation (12), constitué par un moyen de commutation commandé par logiciel.

25 4. Système de communication téléphonique selon une des revendications 1 à 3, caractérisé en ce que le module de radiocommunication (10) comprend au moins une commande du menu affiché, sur un moyen d'affichage du terminal, permettant de choisir le mode de conversation et de transmission.

5. Système de communication téléphonique selon une des revendications 1 à 4, caractérisé en ce que le module de chiffrement / déchiffrement (28) est inséré dans un boîtier capot relié au module terminal par un contacteur (31).

5 6. Système de communication téléphonique selon la revendication 4 ou 5, caractérisé en ce que le module de chiffrement / déchiffrement (28) comporte un lecteur de support de données pour l'échange uniquement de clés de session de chiffrement de l'utilisateur.

10 7. Système de communication téléphonique selon une des revendications 4 à 6, caractérisé en ce que le module de radiocommunication (10) comporte une connexion série (25) vers un modem externe (33).

8. Système de communication téléphonique selon la revendication 7, caractérisé en ce que la connexion série (25) est filaire de type RS232.

15 9. Système de communication téléphonique selon la revendication 7, caractérisé en ce que la connexion série (25) est non filaire.

10. Système de communication téléphonique selon la revendication 9, caractérisé en ce que la connexion série (25) non filaire est Infrarouge.

20 11. Système de communication téléphonique selon la revendication 9, caractérisé en ce que la connexion série (25) non filaire est radio 802.11 (WIFI).

12. Système de communication téléphonique selon la revendication 9, caractérisé en ce que la connexion série (24) non filaire est bluetooth.

25 13. Système de communication téléphonique selon une des revendications 4 à 12, caractérisé en ce que le mode de conversation sélectionné par le menu est une communication téléphonique en clair à travers le réseau de radiotéléphonie cellulaire, mettant en liaison directement un DSP (16) en émission ou en réception avec un circuit de modulation démodulation radio (12) du module de radiocommunication (10).

14. Système de communication téléphonique selon une des revendications 4 à 12, caractérisé en ce que le mode de conversation sélectionné par le menu est une communication téléphonique cryptée à travers le réseau de radiotéléphonie cellulaire, ce mode intercalant par la
5 commutation du premier aiguillage (27) entre un DSP (16) et un circuit de modulation / démodulation radio (12) du module de radiocommunication (10) le module de chiffrement / déchiffrement (28).

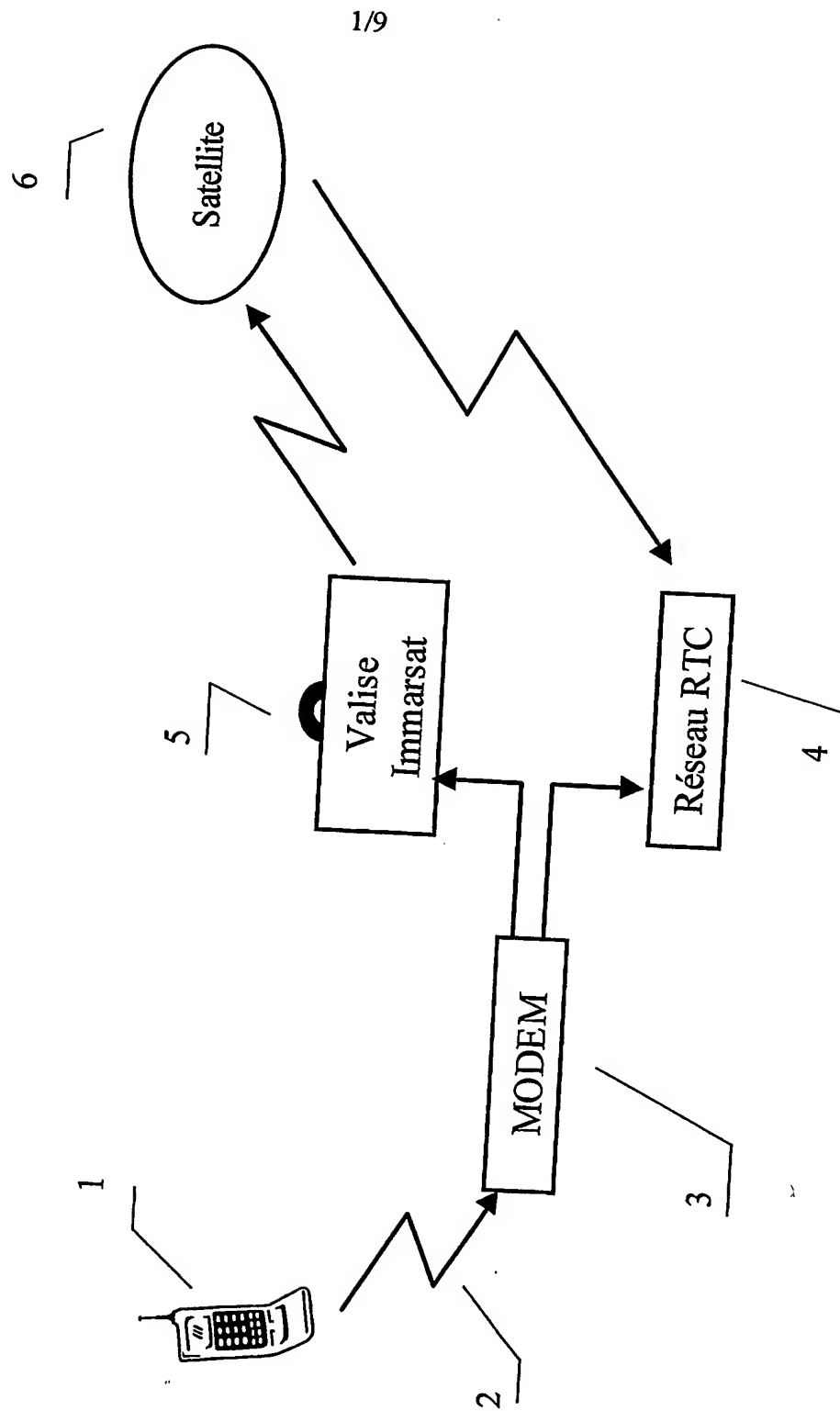
15. Système de communication téléphonique selon une des revendications 4 à 12, caractérisé en ce que le mode de conversation
10 sélectionné par le menu est une communication téléphonique cryptée à travers le réseau de téléphonie commuté (4) ou un satellite (6) via un modem externe (33) commandé par le module de radiocommunication (10), ce mode intercalant, par la commutation du premier aiguillage (27), entre le DSP (16) et le module de chiffrement / déchiffrement (28), un circuit vocodeur (30)
15 adaptant les signaux numériques du DSP (16) à la vitesse de transmission d'un modem avant de les envoyer au circuit de chiffrement / déchiffrement (29) et déroutant les signaux provenant du modem externe (33) en sortant du circuit de chiffrement déchiffrement vers un haut-parleur (13) et ceux provenant d'un microphone (19) et sortant du circuit de
20 chiffrement / déchiffrement (29) vers le modem externe (33).

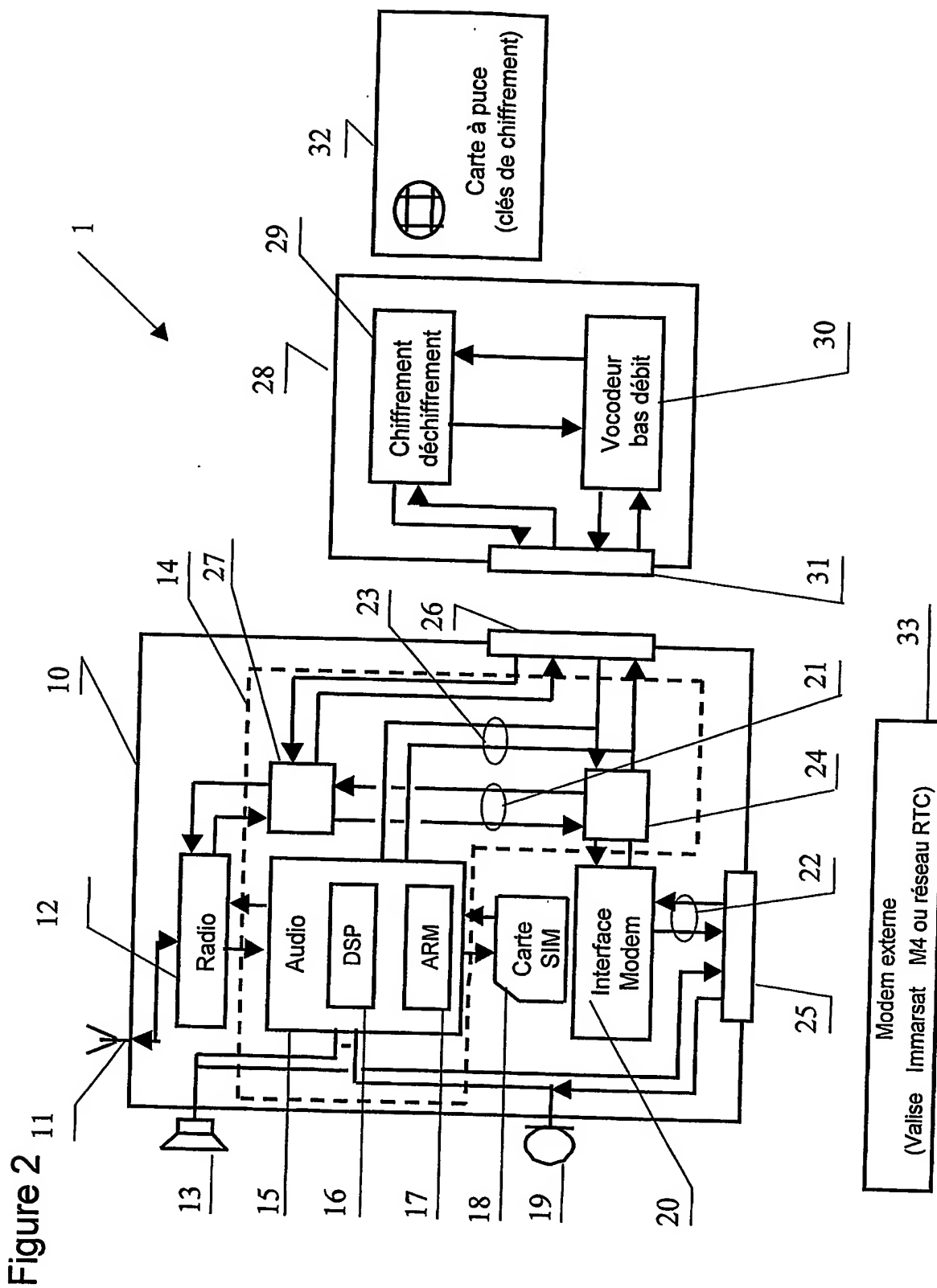
16. Système de communication téléphonique selon une des revendications 4 à 12, caractérisé en ce que le mode de transmission des données sélectionné par le menu est une transmission téléphonique en clair à travers le réseau de radiotéléphonie cellulaire mettant en liaison, par la
25 commutation du second aiguillage (24), le module d'interface modem (20) avec un circuit de modulation démodulation radio (12).

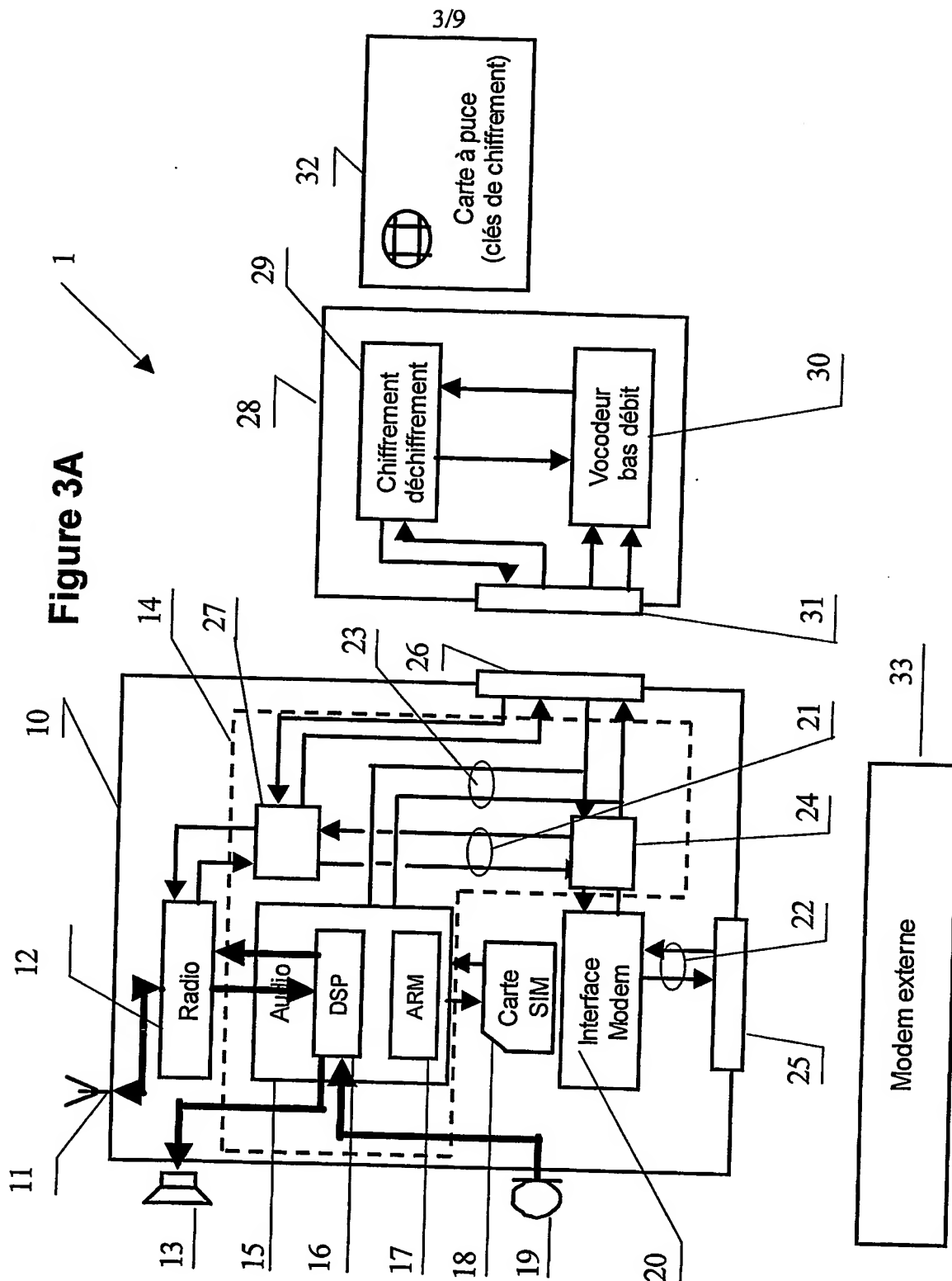
17. Système de communication téléphonique selon une des revendications 4 à 12, caractérisé en ce que le mode de transmission des données sélectionné par le menu est une transmission téléphonique cryptée
30 à travers le réseau de radiotéléphonie cellulaire intercalant, par la commutation du second aiguillage (24), entre le module d'interface modem

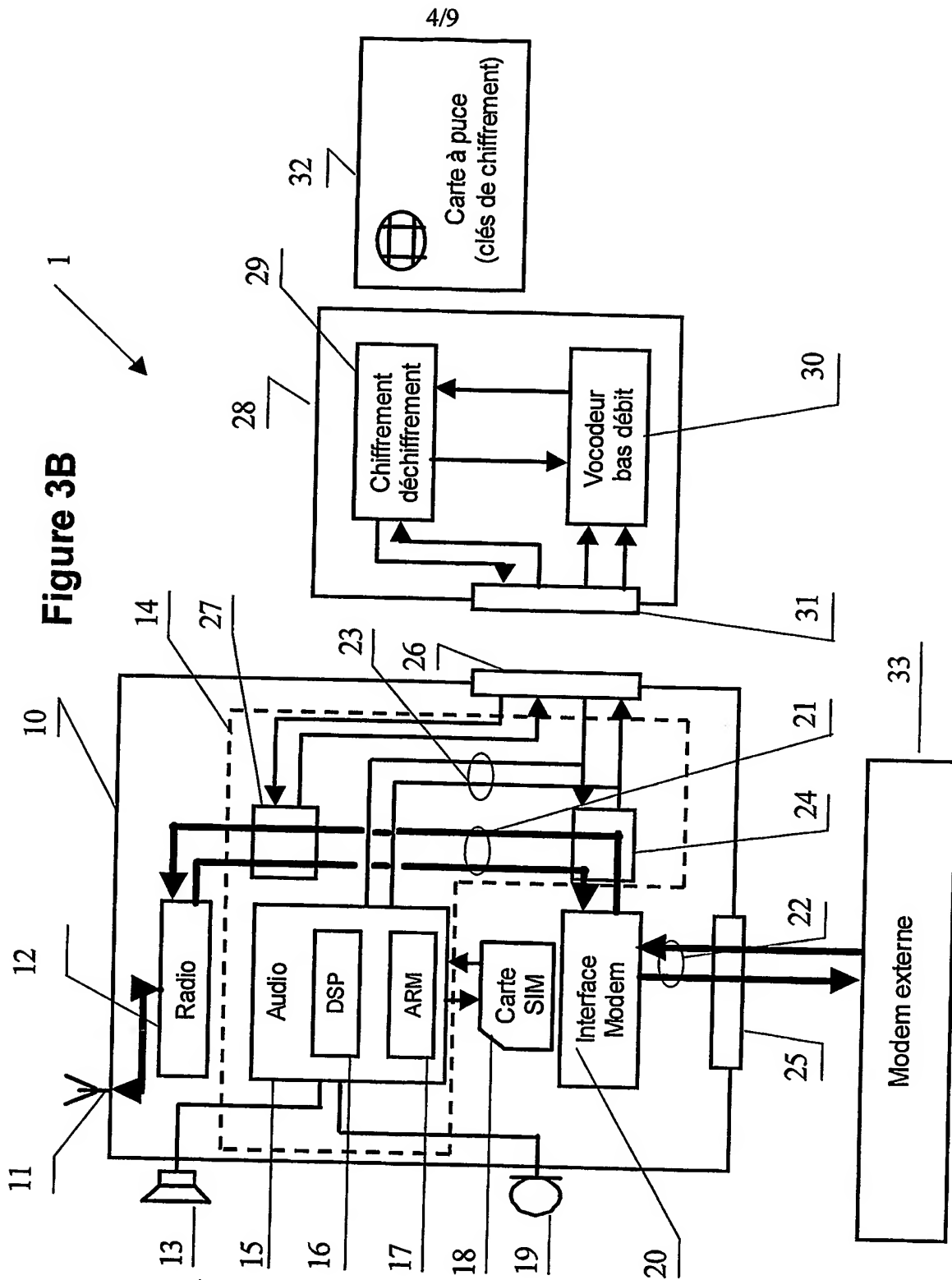
(20) et le circuit de modulation / démodulation radio (12), le module de chiffrement / déchiffrement (28).

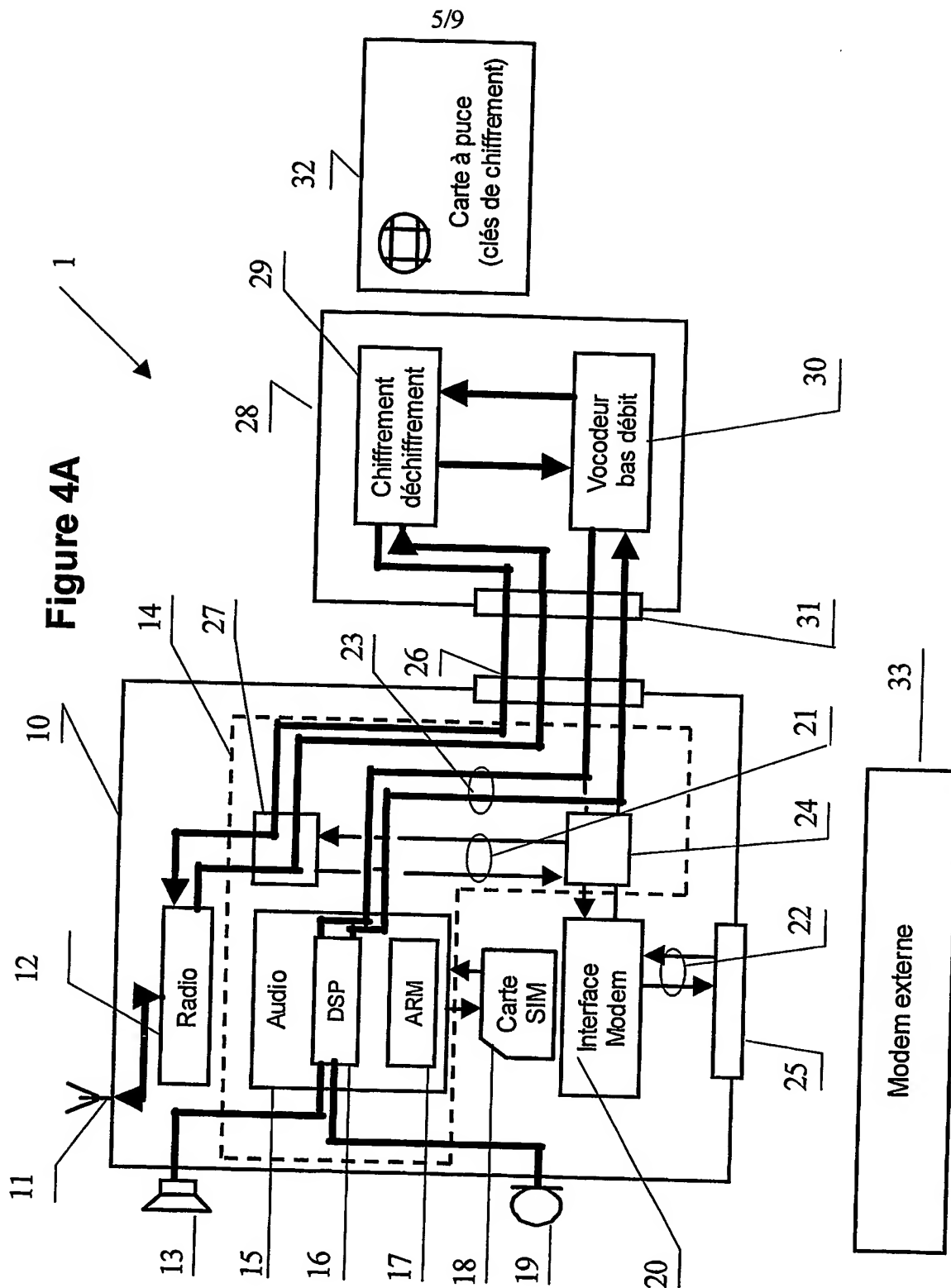
Figure 1

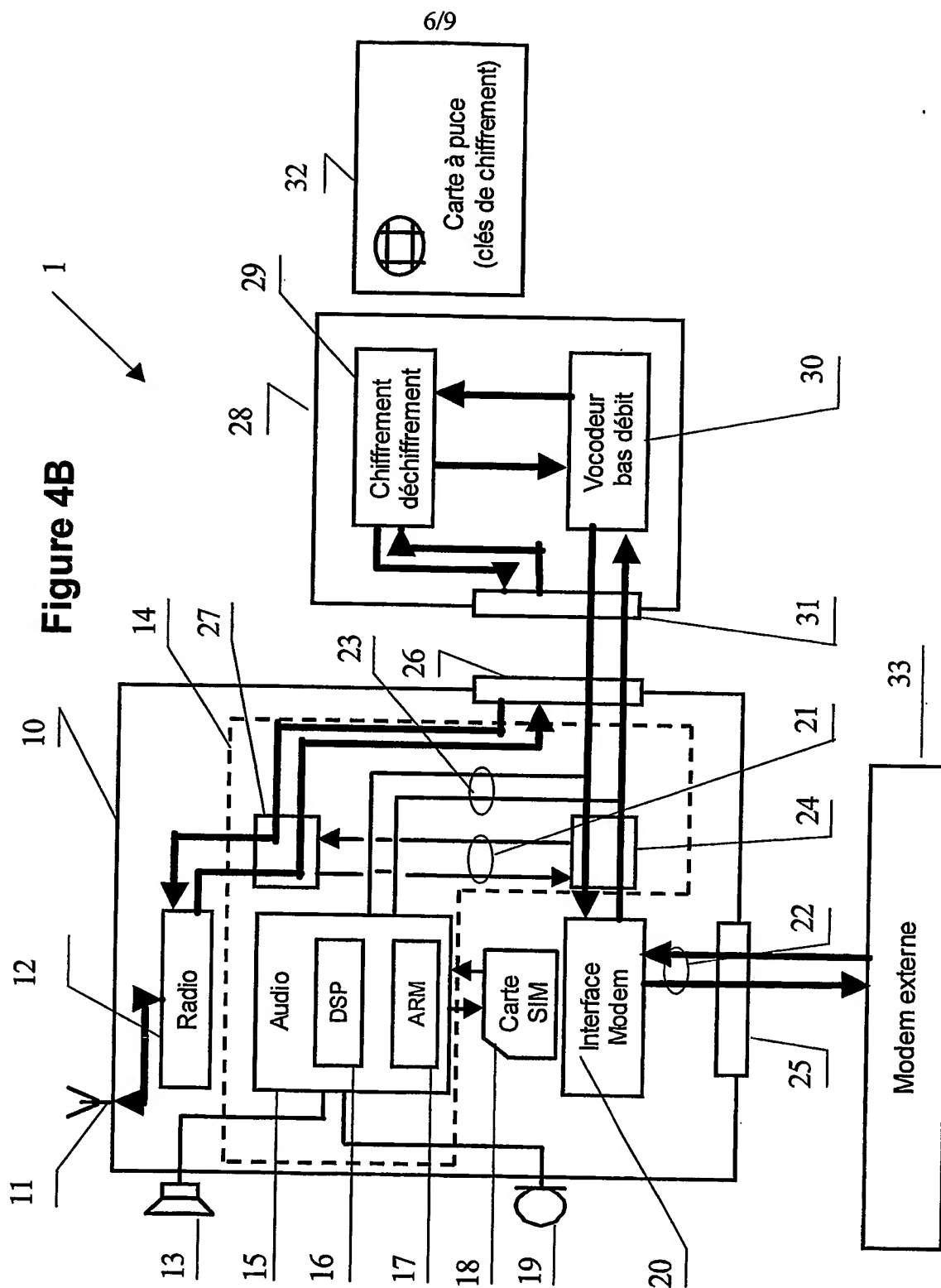


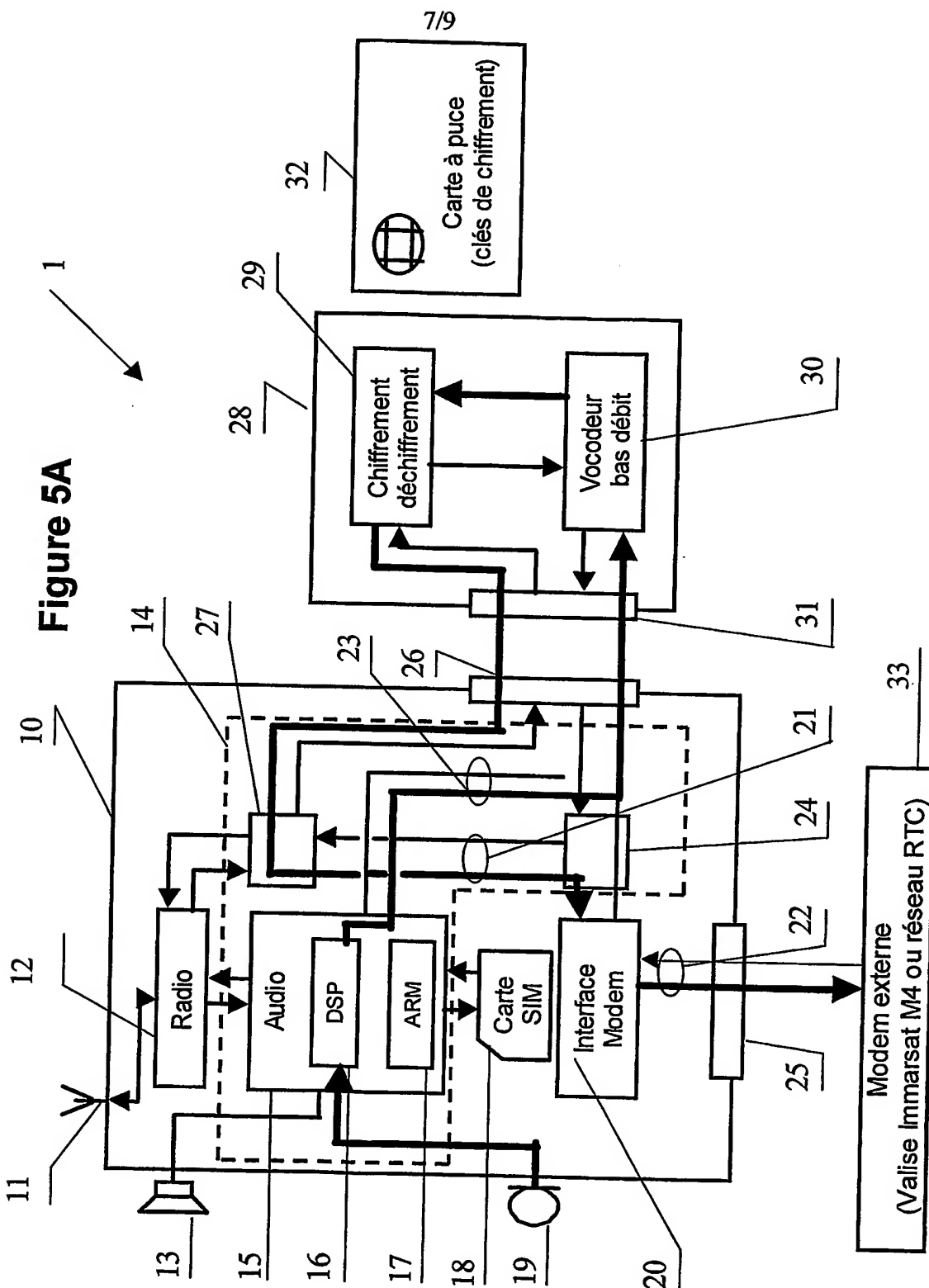












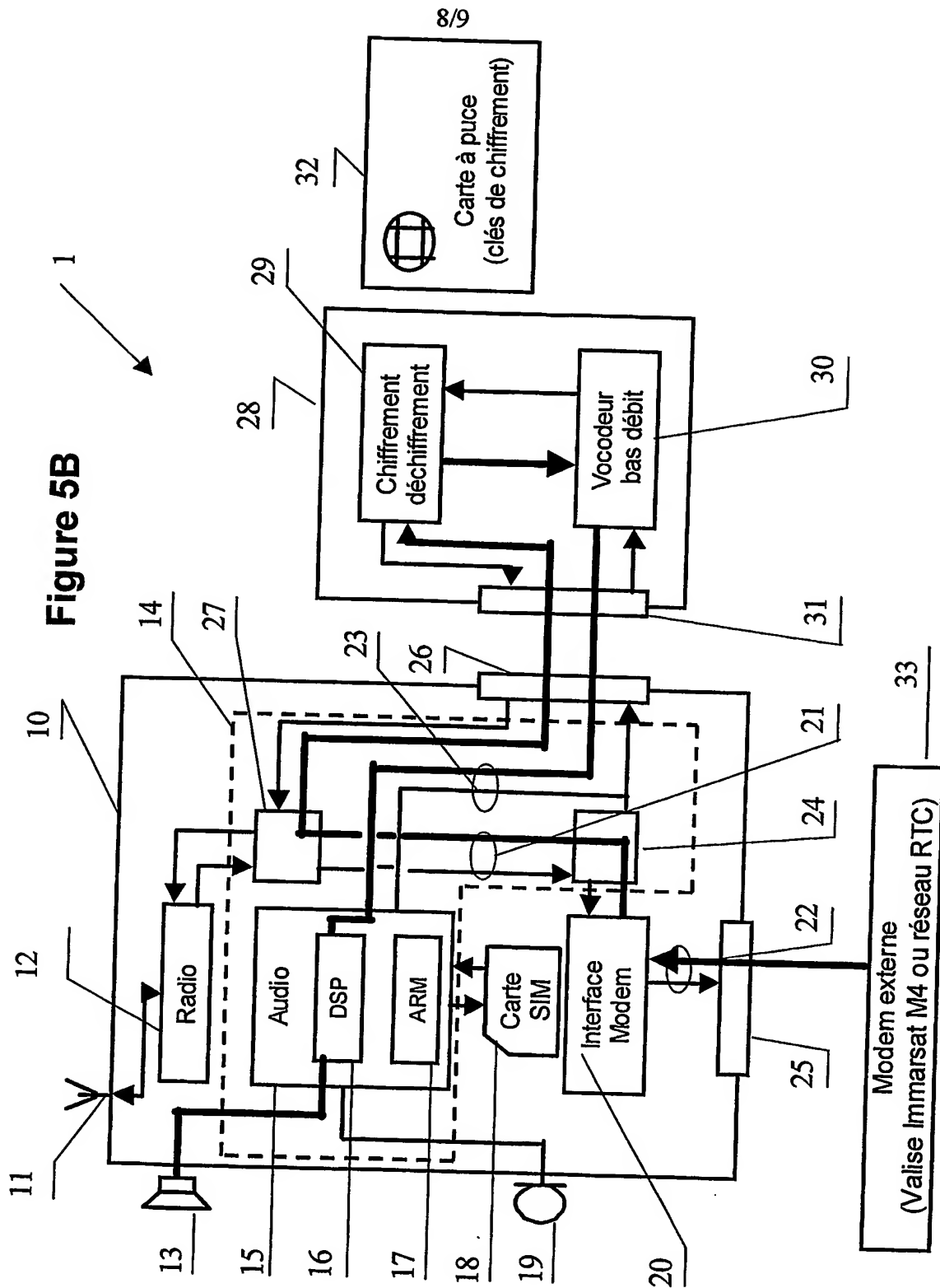


Figure 6

